Incident Response Planning

## The 15 Minute Workgroup Tabletop Exercise

July 2015

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State's security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

1. Modify the tabletop scenario as needed to conform to your environment.

2. Engage management.

3. Present scenario to the workgroup.

4. Discuss the process to address the scenario.

5. Document the response and findings for future reference

Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.
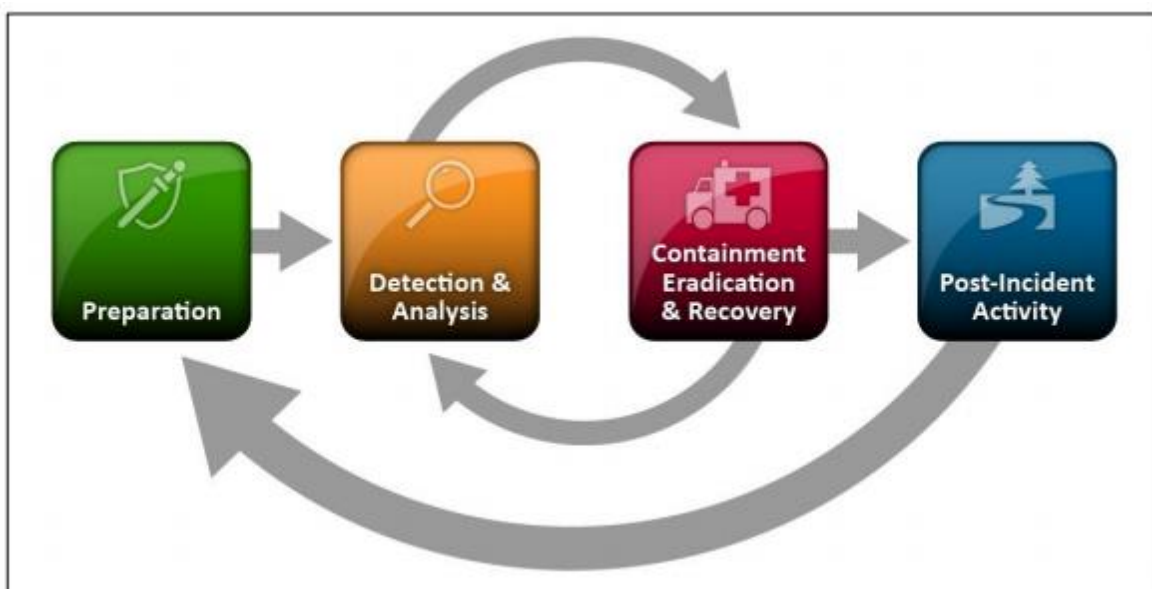
It seems that your website(s) have been having some issues and is periodically losing connectivity. Unfortunately, you are not the only organization to be having problems as the media is reporting that other major organizations have also experienced severe server downtime. Sensing a big story, local news media outlets have started to reach out to your organization asking if the outage of your website(s) is related to the other major outages.

How do you respond?
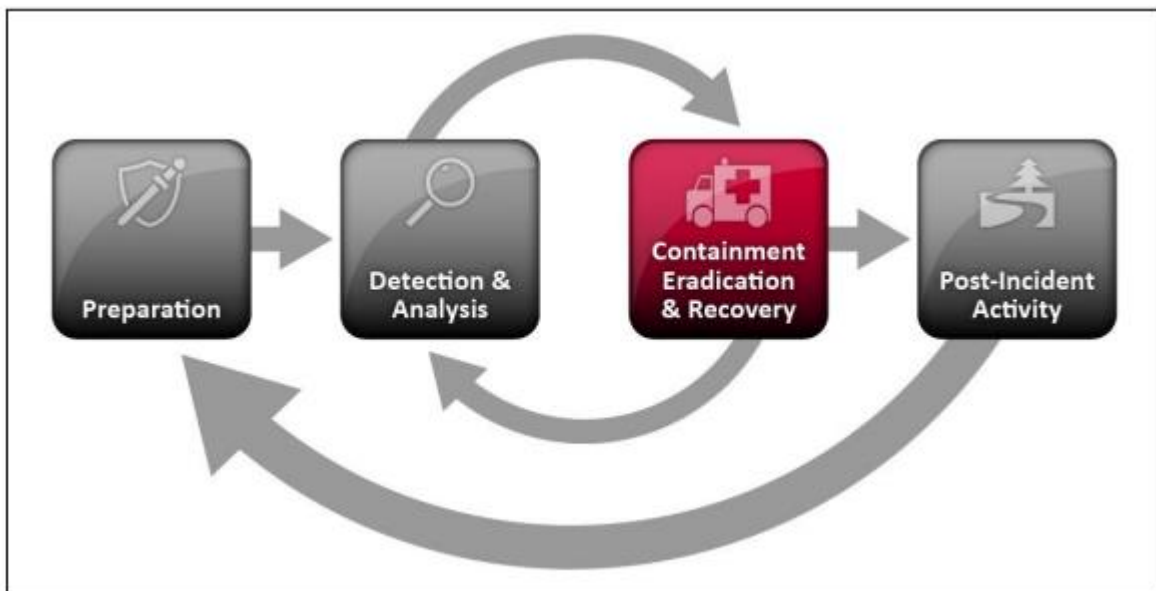
ITEMS TO DISCUSS

- Where would you start?
- What information would you collect about the website(s) outage?
- Where can you find additional information regarding the outages that are impacting the other national organizations?
- Who, within your organization, is responsible for dealing with media inquiries?
- What information do you need to convey to the public?
    - How would you convey it?
- What information needs to be conveyed to your organization's leadership regarding the event and media requests?
    - What information would you share to your organization's staff?
- Does your response change if it was found that you were the victim of a DDoS?
    - Who would you additionally involve in the mitigation?
    - How would the messaging differ?
    - What verbiage can you utilize to provide a simple definition of the event?
- (Alternatively) How does your response change if someone falsely claims via social media to have successfully DDoS'd your organization?

ITEMS TO REPORT

- Did communications flow as expected? If not, why?
- Were processes and procedures followed?
- Were there any surprises?
- How well did the exercise work for your organization?
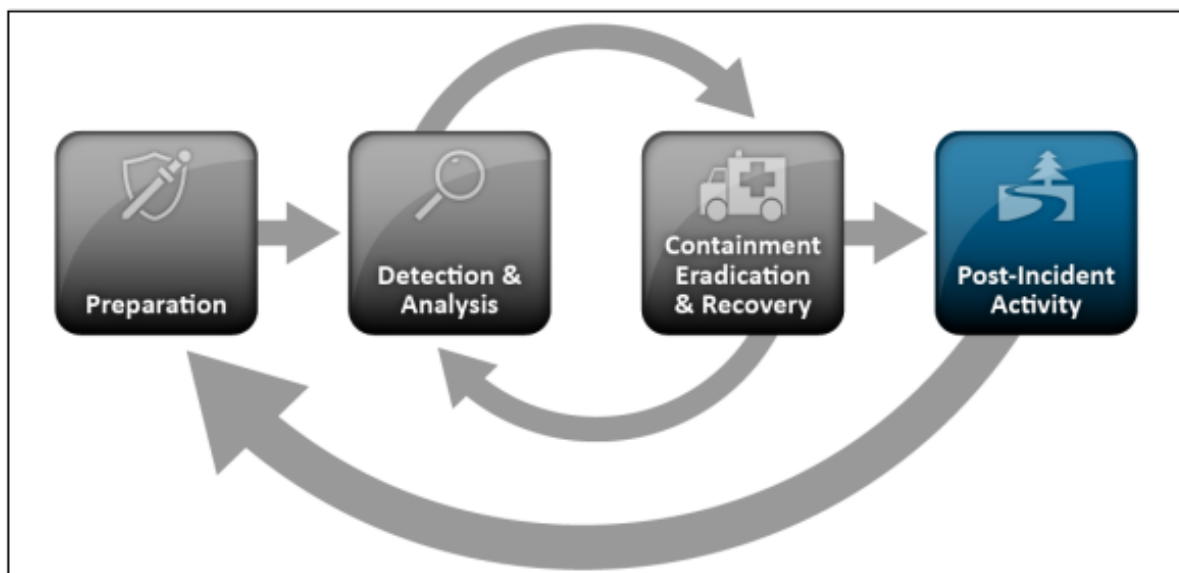
CONTACT US

The State Office of Cyber Security SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

To report a cyber-incident, contact the WaTech Service Desk at (360) 753-2454 / 1-888-241-7597.

For general questions, send us an email at soc@watech.wa.gov.

For more information, visit our site at: http://www.soc.wa.gov.

The State Office of Cyber Security, Security Operations Center (SOC) is an active member with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which has been designated by the US Department of Homeland Security (DHS) as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through this relationship, the State Office of Cyber Security SOC is able to leverage resources available from MS-ISAC of malware analysis, reverse engineering, log analysis, and forensics analysis in a cyber incident.

The mission of the State Office of Cyber Security SOC is to provide centralized information sharing, monitoring, and analysis of Washington State's security posture. The promotion of cyber security education and awareness to end users is critical to maintenance of a strong security posture of the Washington State network.

SECURITY OPERATIONS